M. Anderson Berry (SBN 262879)
aberry@justice4you.com
Gregory Haroutunian (SBN 330263)
gharoutunian@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 239-4778
Fax: (916) 924-1829

Terence R. Coates (*pro hac vice*)
tcoates@msdlegal.com
Justin C. Walker (*pro hac vice*)
jwalker@msdlegal.com
Dylan J. Gould (*pro hac vice*)
dgould@msdlegal.com
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700
Fax: (513) 665-0219

Attorneys for Plaintiffs and the Proposed Class

[Additional counsel on signature page]

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

IN RE: BLACKHAWK NETWORK DATA BREACH LITIGATION	Case No. 3:22-cv-07084-CRB
This Document Relates To:	**AMENDED CONSOLIDATED CLASS ACTION COMPLAINT**
ALL ACTIONS	JUDGE CHARLES R. BREYER
	DEMAND FOR JURY TRIAL

Plaintiffs Steven Pryor, Shane Scheib, Sabrina Singleton, Silvia Cortez, Brian O'Connor, and Kelly Rogers, individually and on behalf of all others similarly situated, bring this Amended Consolidated Class Action Complaint ("Complaint") against Defendant Blackhawk Network, Inc. d/b/a Blackhawk Engagement Solutions ("Blackhawk"" or "Defendant"), a California corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiffs make the following allegations on information and belief, except as to their own actions, which are made on personal knowledge, the investigation of their counsel, and the facts that are a matter of public record.

I. NATURE OF THE ACTION

1. This class action arises out of the recent data breach ("Data Breach") involving Blackhawk, which offers branded payment programs, including prepaid gift cards, to customers.

2. Blackhawk is headquartered in Pleasanton, California.

3. Blackhawk acts as a third-party service provider on behalf of Pathward N.A. ("Pathward"). Pathward uses Blackhawk to activate and manage certain prepaid incentive cards referred to as Pathward Prepaid Cards ("Prepaid Card" or "Prepaid Cards").

4. Blackhawk operates the website www.MyPrepaidCenter.com ("MyPrepaidCenter.com") on behalf of Gift Card holders to activate and manage Pathward's Prepaid Cards. To purchase and use Prepaid Cards, Plaintiffs and Class Members were required to provide certain sensitive, non-public information to Defendant by entering this information on MyPrepaidCenter.com.

5. Unfortunately, Blackhawk failed to properly secure and safeguard the personally identifiable information provided by customers, including Plaintiffs and Class Members, that appeared on the MyPrepaidCenter.com profile, including, without limitation, their unencrypted and unredacted first and last names, email addresses, phone numbers ("PII"), their payment card data in combination with information "related to the Prepaid Card profiles," which included, but was not limited to, information added by customers to PrepaidCenter.com, such as card numbers, expiration dates, and CVV

security codes ("PCD") and other sensitive information (collectively with PII and PCD, "Private Information").[1]

6. On information and belief, this Data Breach was engineered and targeted at accessing and exfiltrating the Private Information of Plaintiffs and Class Members in order for criminals to use that information in furtherance of theft, identity crimes, and fraud.

7. Defendant's failure to prevent and detect the Data Breach is particularly egregious considering the nature of its business and the Private Information it collected, the myriad data breaches all over the country, and its own experience with a substantially similar data breach in 2020, which is described in more detail below. The aggregate information acquired by cybercriminals in this Data Breach is particularly concerning considering that Defendant's customers provided Private Information, which can be used to commit fraud against Plaintiffs and Class Members as well as steal their identities.

8. Plaintiffs bring this class action against Blackhawk to seek damages for themselves and other similarly situated consumers impacted by the Data Breach ("Class Members"), as well as other equitable relief, including, without limitation, injunctive relief designed to protect the sensitive information of Plaintiffs and other Class Members from further data breach incidents.

9. On October 31, 2022, Blackhawk filed a Notice of Data Breach ("Notice") with the Attorney General of Montana. The Notice states, on September 11, 2022, Blackhawk "discovered irregular activity in connection" with MyPrepaidCenter.com.[2] Blackhawk claims it "took prompt steps to investigate the incident, and we stopped the irregular activity on September 12, 2022."[3] In addition,

[1] *Blackhawk Network Notice of Data Breach*, Oct. 31, 2022, archived by the Montana Attorney General, *available at*: https://dojmt.gov/wp-content/uploads/Consumer-Notification-Letter-675.pdf (last accessed Feb. 8, 2023).
[2] *Id.*
[3] *Id.*

Blackhawk states the "unauthorized acquisition occurred between September 4-12, 2022."[4] The Notice provided to the Montana Attorney General is as follows:

> **What Happened?**
>
> On September 11, 2022, we discovered irregular activity in connection with www.MyPrepaidCenter.com, the website that Blackhawk operates for cardholders to activate and manage Pathward Prepaid Cards. We took prompt steps to investigate the incident, and we stopped the irregular activity on September 12, 2022. Our investigation revealed that the irregular activity involved unauthorized acquisition of information about you described below. The unauthorized acquisition occurred between September 4–12, 2022.
>
> **What Information Was Involved?**
>
> This incident involved information you provided for your www.MyPrepaidCenter.com profile, including your first and last name, email address, and phone number (if any). It also included information relating to your Pathward Prepaid Card(s) you added to your www.MyPrepaidCenter.com profile, such as card numbers, expiration dates, and CVV codes.

10. Also, on October 31, 2022, through its attorney, Pathward filed a similar Notice of Data Breach ("Pathward Notice") with the Attorney General of Iowa. The Notice, states that Blackhawk "discovered irregular activity in connection" with MyPrepaidCenter.com.[5]

11. As a result of Defendant's failure to prevent the Data Breach, or detect it during its occurrence, thousands of MyPrepaidCenter.com customers across the United States are suffering and will continue to suffer real and imminent harm as a direct consequence of Defendant's conduct, which includes: (a) refusing to take adequate and reasonable measures to ensure its data systems were protected; (b) refusing to take available steps to prevent the breach from happening; (c) failing to adequately audit and monitor its third party data security vendors; (d) failing to disclose to its customers the material fact that it or its vendors did not have adequate computer systems and security practices to safeguard

[4] *Id.*

[5] *Pathward, N.A. Data Security Incident*, archived by the Iowa Attorney General, *available at*: https://www.iowaattorneygeneral.gov/media/cms/10312022_Blackhawk_Engagement_Solut_1D9CB60967722.pdf (last accessed Feb. 8, 2023).

customers' personal and financial information; and (e) failing to provide timely and adequate notice of the data breach.

12. The injuries suffered by Plaintiffs and Class Members as a direct result of the Data Breach include, *inter alia*:

a. Unauthorized charges on their payment card accounts;

b. Theft of their personal and financial information;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. Loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit, including decreased credit scores and adverse credit notations;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the data breach;

f. The present and continuing injury flowing from potential theft, fraud, and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted to Blackhawk for the sole purpose of using Blackhawk's services and with the mutual

understanding that Blackhawk would safeguard Plaintiffs' and Class Members' Private Information against theft and not allow access to and misuse of their information by others;

h. Money paid to Blackhawk during the period of the Data Breach in that Plaintiffs and Class Members would not have used Blackhawk's services or products, or would have paid less for their services or products, had Defendant disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' Private Information and had Plaintiffs and Class Members known that Blackhawk would not provide timely and accurate notice of the Data Breach; and,

i. Continued risk to their PII and PCD, which remains in the possession of Blackhawk and its vendors, and which is subject to further breaches so long as Blackhawk continues to fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data in its possession.

13. Examples of the harms experienced by Blackhawk customers as a direct and foreseeable consequence of its conduct include the experiences of the representative Plaintiffs described below.

II. THE PARTIES

Plaintiff Steven Pryor

14. Plaintiff Steven Pryor is a citizen of the State of Colorado and a resident of Johnstown, Colorado. Plaintiff Pryor is the owner of two payment cards serviced by MyPrepaidCenter.com. Plaintiff Pryor received a Notice of Data Breach dated October 31, 2022, by U.S. Mail.

Plaintiff Shane Scheib

15. Plaintiff Shane Scheib is a citizen of the State of Mississippi and a resident of Canton, Mississippi. Plaintiff Scheib is the owner of two payment cards serviced by MyPrepaidCenter.com. Plaintiff Scheib received a Notice of Data Breach dated October 31, 2022, by U.S. Mail.

Plaintiff Sabrina Singleton

16. Plaintiff Sabrina Singleton is a resident and citizen of the State of New York and a resident of Auburn, New York. Plaintiff Singleton had at least one Prepaid Card serviced by Blackhawk on MyPrepaidCenter.com. Plaintiff Singleton received a Notice of Data Breach dated October 31, 2022, U.S. Mail.

Plaintiff Silvia Cortez

17. Plaintiff Silvia Cortez is a citizen of the State of Texas and a resident of Houston, Texas. Plaintiff Cortez had at least one Prepaid Card serviced by Blackhawk on MyPrepaidCenter.com. Plaintiff Cortez received a Notice of Data Breach dated October 31, 2022, by U.S. Mail.

Plaintiff Brian O'Connor

18. Plaintiff Brian O'Connor is a citizen of the State of California and a resident of Rancho Santa Fe, California. Plaintiff O'Connor had at least one Prepaid Card serviced by Blackhawk on MyPrepaidCenter.com. Plaintiff O'Connor received a Notice of Data Breach dated October 31, 2022, by U.S. Mail.

Plaintiff Kelly Rogers

19. Plaintiff Kelly Rogers is a citizen of the State of Illinois and a resident of Wheaton, Illinois. Plaintiff Rogers had three Prepaid Card serviced by Blackhawk on MyPrepaidCenter.com. Plaintiff Rogers received a Notice of Data Breach dated October 31, 2022, by U.S. Mail.

Defendant Blackhawk

20. Defendant is a privately held corporation incorporated in the State of California. Defendant's headquarters is located at 6220 Stoneridge Mall Road, Pleasanton, California 94588. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

21. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. §1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

22. This Court has personal jurisdiction over Defendant because Defendant and/or its parents or affiliates are headquartered in this District and Defendant conducts substantial business in California and this District through its headquarters, offices, parents, and affiliates.

23. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

24. Blackhawk is primarily engaged in providing "global branded payments" to its customers located within the United States and abroad, which includes gift cards, prepaid incentive cards, other online payment options for employers and merchants, gaming, and gambling options.[6] Blackhawk is a privately held company with corporate headquarters in Pleasanton, California.

25. Blackhawk operates a consumer facing website located at www.blackhawknetwork.com ("Blackhawknetwork.com"). Customers or potential customers can then access MyPrepaidCenter.com through Blackhawknetwork.com.

26. To activate or access a prepaid card on MyPrepaidCenter.com a customer must provide certain Private Information. It is specified in the Blackhawk Network Privacy Notice ("Privacy Notice")

[6] Blackhawk Network Website, *available at*: https://blackhawknetwork.com/ (last accessed on Feb. 8, 2023).

that the policy pertains to all visitors, customers, users of apps, and users of gift card and banded payments. Specifically, the Private Information, which Defendant collects, includes, but is not limited to:

- Contact information, such as name, email address, mailing address, fax, or phone number;
- Payment and financial information, such as credit or other payment card information, bank account, or billing address;
- Shipping address and related details;
- Resume, employment and education history, name and contact details, background details, and references when you apply to job postings or contact us about employment opportunities;
- Company and employment information;
- Subject to applicable local law restrictions, Social Security number or other national tax ID number (for clients and potential clients);
- Unique identifiers such as username, account number, or password;
- Preference information such as product wish lists, order history, or marketing preferences;
- Information about businesses, such as company name, size, or business type; and
- Demographic information, such as age, gender, interests and ZIP or postal code.[7]

27. Defendant also specifies in the Privacy Policy that it acts as the "Controller" of the Private Information supplied.

28. When they provided their Private Information to Defendant, Plaintiffs and Class Members relied on Defendant (a large, sophisticated internet retailer) to keep their Private Information confidential

[7] *Blackhawk Network Privacy Notice*, quoting, "Personal Information we Collect" *available at*: https://blackhawknetwork.com/privacy-policy (last accessed on Feb. 8, 2023).

and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

29. Defendant had a duty to take reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to unauthorized third parties. This duty is inherent in the nature of the exchange of the highly sensitive Private Information at issue here, particularly where digital transactions are involved.

30. Defendant also recognized and voluntarily adopted additional duties to protect PII and PCD in its Privacy Policy which has been publicly posted to the internet.[8] In its Privacy Policy, Defendant also says the way it uses Private Information is at "the core of our obligations," that it will "not sell" information, and that it will use the information for "our own legitimate and lawful business interests."[9]

31. Despite these duties and promises, Defendant allowed data thieves to infect and infiltrate its MyPrepaidCenter.com website and steal the Private Information of thousands of its customers.

The Data Breach was foreseeable

32. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[10]

33. In light of recent high profile data breaches at other industry leading companies, including Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or

[8] *Id.*

[9] *Id.*

[10] Bree Fowler, *Data breaches break record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/#:~:text=The%20number%20of%20reported%20data%20breaches%20jumped%2068%20percent%20last,of%201%2C506%20set%20in%202017. (last accessed Feb. 8, 2023).

should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

34. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of and may therefore take appropriate measures to prepare for (or thwart) such an attack.

35. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgment of its duties to keep Private Information confidential and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and the Class from being compromised.

The Data Breach

36. On or about October 31, 2022, Defendant notified various state Attorneys General, as well as Plaintiffs and Class Members that, on September 12, 2022, Defendant discovered that MyPrepaidCenter.com experienced "irregular activity."[11]

37. The Notice informed Plaintiffs and Class Members that "Our investigation revealed that irregular activity involved the unauthorized acquisition of information about you." This information included first and last name, email address, and phone numbers, but it also included information relating to the Pathward Prepaid Card(s), added on the MyPrepaidCenter.com profile such as card numbers, expiration dates, and CVV security codes.[12]

38. The Private Information exfiltrated in the Data Breach was unencrypted and captured directly from MyPrepaidCenter.com.[13]

---

[11] *Blackhawk Network Notice of Data Breach*, Oct. 31, 2022, archived by the Iowa Attorney General, *available at*: https://www.iowaattorneygeneral.gov/media/cms/10312022_Blackhawk_Engagement_Solut_1D9CB60967722.pdf (last accessed Feb. 8, 2023).

[12] *Id.*

[13] *Id.*

39. Defendant claims it "blocked your impacted Pathward Prepaid Card(s)," yet it remained silent about what happened to the stolen Personal Information.[14]

40. Despite Defendant's promises that it: (i) would not disclose consumers' Private Information to unauthorized third parties; and (ii) would protect consumers' Private Information with adequate security measures, it appears that Defendant did not even implement, or require its third-party vendors to implement, basic security measures such as immediately encrypting PCD. This negligence imposes risks to Plaintiffs and Class Members that they must endure for the foreseeable future.

Blackhawk Experienced a Substantially Similar Data Breach Two Years Earlier

41. According to an earlier Security Incident Notification ("Notification"), on August 8, 2020, Blackhawk "detected some activity on its website GiftCards.com, indicating a possible 'brute force attack.'"[15]

42. Blackhawk conducted an investigation on August 14, 2020 and determined that the incident resulted in "unauthorized access" to a number of accounts.[16]

43. The Notification also indicates similar Private Information was taken in the 2020 data breach as was taken in the Data Breach that is the subject of this class action:

> For any account accessed, the perpetrator(s) would have only had access to the customer's transaction history, original balance information for gift card(s), and account profile information, which includes customer name, email address, postal address, the name and contact information of any gift card recipient(s), and the last four digits of the credit card used in prior transactions. The perpetrator(s) would not have been able to access the full numbers of any gift cards purchased or the credit cards used to purchase gift cards through customer accounts. Further, the perpetrator(s) would not have been able to initiate a transaction using any stored cards without the Card Identification Number (CID) code for the particular credit card (which would not have been accessible through GiftCard.com).[17]

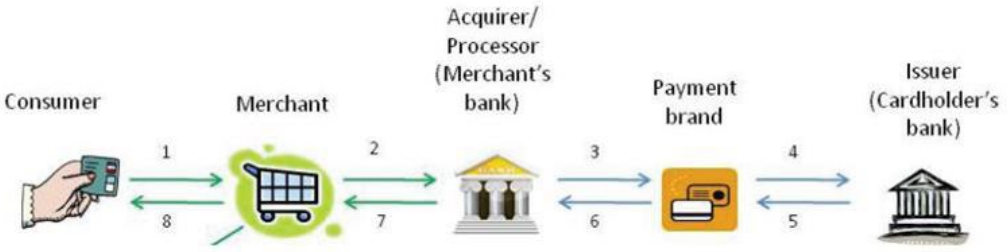
---

[14] *Id.*
[15] *Blackhawk Security Incident Notification*, August 28, 2020, archived at the Maryland Attorney General, *available at:* https://www.marylandattorneygeneral.gov/ID%20Theft%20Breach%20Notices/2020/itu-331656.pdf (last accessed on Feb. 8, 2023).
[16] *Id.*
[17] *Id.*

Securing PII and Preventing Breaches

44. Given Blackhawk's recent experience with data breaches, it should have been even more aware and taken further precautions to secure PII and other private information.

45. In a debit or credit card purchase transaction, card data must flow through multiple systems and parties to be processed. Generally, the cardholder presents a credit or debit card to an e-commerce retailer (through an e-commerce website) to pay for merchandise. The card is then "swiped," and information about the card and the purchase is stored in the retailer's computers and then transmitted to the acquirer or processor (*i.e.*, the retailer's bank). The acquirer relays the transaction information to the payment card company, who then sends the information to the issuer (*i.e.*, cardholder's bank). The issuer then notifies the payment card company of its decision to authorize or reject the transaction. *See* graphic below:[18]



1	The consumer selects a card for payment. The cardholder data is entered into the merchant's payment system, which could be the point-of-sale (POS) terminal/software or an e-commerce website.
2	The card data is sent to an acquirer/payment processor, whose job it is to route the data through the payments system for processing. With e-commerce transactions, a "gateway" provider may provide the link from the merchant's website to the acquirer.
3	The acquirer/processor sends the data to the payment brand (e.g. Visa, MasterCard, American Express, etc.) who forward it to the issuing bank/issusing bank processor
4	The issuing bank/processor verifies that the card is legitimate, not reported lost or stolen, and that the account has the appropriate amount of credit/funds available to pay for the transaction.
5	If so, the issuer generates an authorization number and routes this number back to the card brand. With the authorization, the issuing bank agrees to fund the purchase on the consumer's behalf.
6	The card brand forwards the authorization code back to the acquirer/processor.
7	The acquirer/processor sends the authorization code back to the merchant.
8	The merchant concludes the sale with the customer.

[18] *Payments 101: Credit and Debit Card Payments*, FIRST DATA, at 7 (Oct. 2010), http://euro.ecom.cmu.edu/resources/elibrary/epay/Payments-101.pdf (last accessed Feb. 8, 2023).

46. There are two points in the payment process where sensitive cardholder data is at risk of being exposed or stolen: pre-authorization when the merchant has captured a consumer's data and it is waiting to be sent to the acquirer; and post-authorization when cardholder data has been sent back to the merchant with the authorization response from the acquirer and placed into storage in merchant's servers.

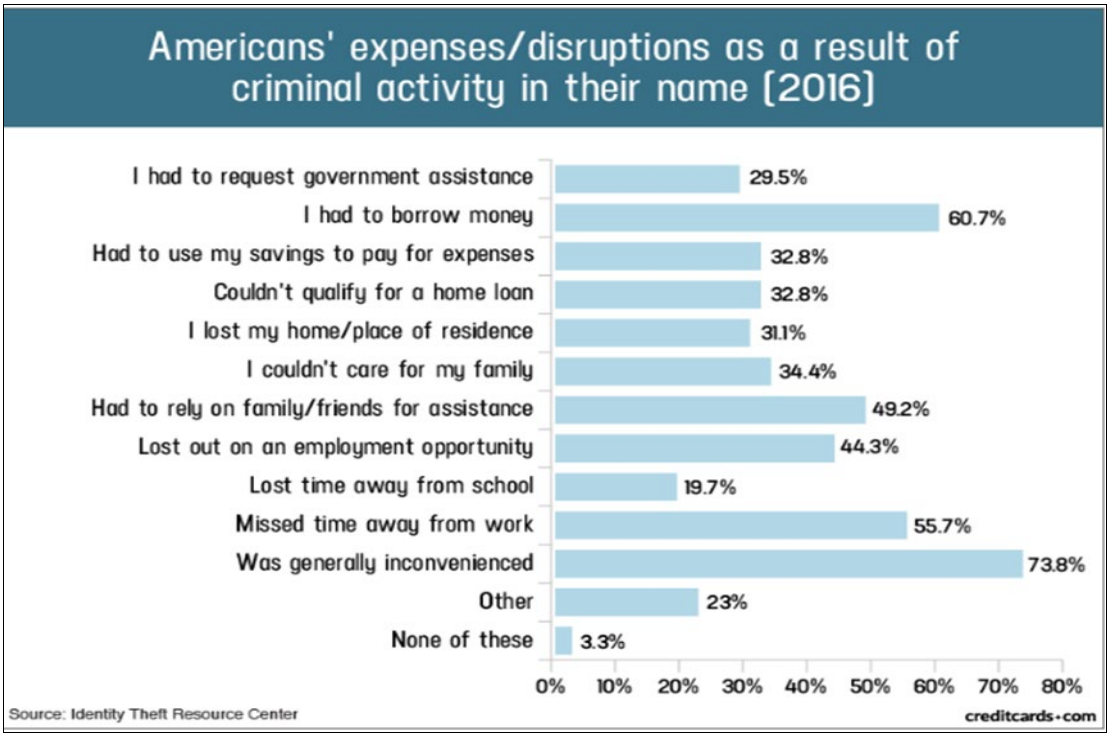
47. Encryption mitigates security weaknesses that exist when cardholder data has been stored, but not yet authorized, by using algorithmic schemes to transform plain text information into a non-readable format called "ciphertext." By scrambling the payment card data the moment it is "swiped," hackers who steal the data are left with useless, unreadable text in the place of payment card numbers accompanying the cardholder's personal information stored in the retailer's computers. Blackhawk failed to implement such a simple solution, which would have protected its customers' data.

48. The financial fraud suffered by Plaintiffs and other customers demonstrates that Defendant , and/or its third party vendors, chose not to invest in the technology to encrypt payment card data (PCD) at point-of-sale to make its customers' data more secure; failed to install updates, patches, and malware protection or to install them in a timely manner to protect against a data security breach; and/or failed to provide sufficient control of employee credentials and access to computer systems to prevent a security breach and/or theft of PCD.

49. These failures demonstrate a clear breach of the Payment Card Industry Data Security Standards (PCI DSS), which are industry-wide standards for any organization that handles PCD.

50. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of Private Information:[19]

[19] Jason Steele, *Credit Card Fraud and ID Theft Statistics,* CREDITCARDS.COM (June 11, 2021), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last accessed Feb. 8, 2023) [https://web.archive.org/web/20200918073034/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/].



51. Plaintiffs and Class Members have experienced one or more of these harms as a result of the data breach.

52. Furthermore, theft of Private Information is also gravely serious. Private Information is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

53. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that

> attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

54. Private Information and PCD are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

55. There is a strong probability that entire batches of stolen payment card information have been dumped on the black market or are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts for many years to come.

56. Plaintiffs and Class Members have suffered and will continue to suffer injuries as a direct result of the Data Breach. In addition to fraudulent charges and damage to their credit, many victims spent substantial time and expense relating to:

a. Finding fraudulent charges;
b. Canceling and reissuing cards;
c. Purchasing credit monitoring and identity theft prevention;
d. Addressing their inability to withdraw funds linked to compromised accounts;
e. Removing withdrawal and purchase limits on compromised accounts;
f. Taking trips to banks and waiting in line to obtain funds held in limited accounts;
g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;
h. Resetting automatic billing instructions; and
i. Paying late fees and declined payment fees imposed as a result of failed automatic payments.

[20] U.S. Gov't Accountability Off., GAO 07737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last accessed Feb. 8, 2023).

57. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

58. Plaintiffs' and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

59. As a direct and proximate result of the Data Breach, Plaintiffs' Private Information was "skimmed" and exfiltrated and is in the hands of identity thieves and criminals, as evidenced by the fraud perpetrated against Plaintiffs and Class Members.

60. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been placed at an immediate and continuing increased risk of harm from fraud. Plaintiffs and Class Members now have to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing, or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

61. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

62. Plaintiffs and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in similar cases.

63. Plaintiffs and Class Members were also damaged via benefit-of-the-bargain damages. The implied contractual bargain entered into between Plaintiffs and Defendant included Defendant's contractual obligation to provide adequate data security, which Defendant failed to provide. Thus, Plaintiffs and the Class Members did not get what they paid for.

64. Plaintiffs and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

65. Plaintiffs and Class Members have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Trespass, damage to and theft of their personal property including Private Information;

b. Improper disclosure of their Private Information;

c. The present and continuing injury flowing from potential fraud and identity theft posed by customers' Private Information being placed in the hands of criminals;

d. Damages flowing from Defendant's untimely and inadequate notification of the Data Breach;

e. Loss of privacy suffered as a result of the Data Breach;

f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. Ascertainable losses in the form of deprivation of the value of customers' Private Information for which there is a well-established and quantifiable national and international market; and,

h. The loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money customers were permitted to obtain from their accounts.

66. The substantial delay in providing notice of the Data Breach deprived Plaintiffs and the Class Members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach. As a result of Defendant's delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiffs and Class Members was and has been driven even higher.

Value of Personal Identifiable Information

67. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[21] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[22] Criminals can also purchase access to entire company data breaches from $900 to $4,500.

68. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[23] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[24] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[25]

69. As a result of the Data Breach, Plaintiffs', and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its acquisition by cybercriminals. This transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private

---

[21] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed on Feb. 8, 2023).

[22] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed on Feb. 8, 2023).

[23] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LOS ANGELES TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed on Feb. 8, 2023).

[24] See Data Coup, https://datacoup.com/ (last accessed on Feb. 8, 2023).

[25] *Frequently Asked Questions*, Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed Feb. 8, 2023).

Information is likely readily available to others, and the rarity of the Private Information has been destroyed, thereby causing additional loss of value.

70. The fraudulent activity resulting from the Data Breach may not come to light for years and Plaintiffs and Class Members face a risk of fraud and identity theft as a result of the Data Breach.

71. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, particularly given the sensitive nature of their purchases, and of the foreseeable consequences that would occur if Defendant's data security system was breached (as it had been as recently as 2020), including, specifically, the significant costs and risks that would be imposed on Plaintiffs and Class Members as a result of a breach.

72. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

73. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's storage platform, amounting to tens or hundreds of thousands of individuals' detailed, Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

74. To date, Defendant has offered no credit monitoring or identity theft services. It has only offered to provide replacement Pathway Prepaid Cards. This is wholly inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the Private Information at issue here.

75. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures, and failure to adequately

investigate, monitor, and audit its third-party vendors, to protect the Private Information of Plaintiffs and Class Members.

A. PLAINTIFFS' EXPERIENCE

Plaintiff Steven Pryor's Experience

76. Plaintiff Pryor was required to provide Defendant with his Private Information to access or activate his prepaid payment cards on Defendant's MyPrepaidCenter.com website.

77. Plaintiff Pryor suffered actual injury from having his Private Information compromised and/or stolen as a result of the Data Breach.

78. Plaintiff Pryor suffered actual injury and damages in paying money to and using services from Defendant during the Data Breach that he would not have paid or ordered had Defendant disclosed that it lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Defendant provided timely and accurate notice of the Data Breach.

79. Plaintiff Pryor suffered actual injury in the form of damages to and diminution in the value of his personal and financial information – a form of intangible property that the Plaintiff Pryor entrusted to Defendant for the purpose of making purchases on its website and which was compromised in, and as a result of, the Data Breach.

80. Plaintiff Pryor suffers present and continuing injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his personal and financial information being placed in the hands of criminals who have already misused such information stolen in the Data Breach.

81. Plaintiff Pryor has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected, and safeguarded from future breaches.

82. As a result of the Data Breach, Plaintiff Pryor made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach; reviewing credit

reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff Pryor has spent several hours dealing with the Data Breach, valuable time Plaintiff Pryor otherwise would have spent on other activities.

83. As a result of the Data Breach, Plaintiff Pryor has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity crimes, fraud, and theft. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

84. Plaintiff Pryor suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff Pryor; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

85. As a result of the Data Breach, Plaintiff Pryor anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Pryor is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Shane Scheib's Experience

86. Plaintiff Scheib was required to provide Defendant with his Private Information to access or activate his prepaid payment cards on Defendant's MyPrepaidCenter.com website.

87. Plaintiff Scheib suffered actual injury from having his Private Information compromised and/or stolen as a result of the Data Breach.

88. Plaintiff Scheib owned two prepaid payment cards maintained and serviced on Defendant's MyPrepaidCenter.com website.

89. On or around September 10, 2022, cyber criminals made two fraudulent transactions from Plaintiff Scheib's accounts, stealing $451.65 from Plaintiff Scheib's digital prepaid Mastercard and $10.82 from Plaintiff's Scheib's prepaid Visa card.

90. Plaintiff Scheib was not reimbursed for his stolen property until December 15, 2022.

91. Plaintiff Scheib suffered actual injury in the form of fraudulent charges on his prepaid payment cards and the loss of use of funds while disputing the unauthorized charge and additional damages resulting from such loss of use.

92. Plaintiff Scheib was not reimbursed for the loss of use, loss of access to, or restrictions placed upon his account that occurred as a result of the Data Breach.

93. Plaintiff Scheib suffered actual injury and damages in paying money to and using services from Defendant during the Data Breach that he would not have paid or ordered had Defendant disclosed that it lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Defendant provided timely and accurate notice of the Data Breach.

94. Plaintiff Scheib suffered actual injury in the form of damages to and diminution in the value of his personal and financial information – a form of intangible property that the Plaintiff Scheib entrusted to Defendant, and which was compromised in, and as a result of, the Data Breach.

95. Plaintiff Scheib suffers present and continuing injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his personal and financial information being placed in the hands of criminals who have already misused such information stolen in the Data Breach.

96. Plaintiff Scheib has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected, and safeguarded from future breaches.

97. As a result of the Data Breach, Plaintiff Scheib made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching the Data Breach; contacting Defendant multiple times to report that his funds on his prepaid cards were accessed and stolen; filling out extensive paperwork to report the theft of his funds; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant; and paying out-of-pocket $140 a year for ID protection services. Plaintiff Scheib has spent more than 10 hours so far dealing with the Data Breach, valuable time Plaintiff Scheib otherwise would have spent on other activities.

98. As a result of the Data Breach, Plaintiff Scheib has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity crimes, fraud, and theft. Plaintiff is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

99. Plaintiff Scheib suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Scheib; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

100. As a result of the Data Breach, Plaintiff Scheib anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Scheib is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Kelly Rogers' Experience

101. Plaintiff Rogers was required to provide Defendant with her Private Information to access or activate her prepaid payment cards on Defendant's MyPrepaidCenter.com website.

102. Plaintiff Rogers suffered actual injury from having her Private Information compromised and/or stolen as a result of the Data Breach.

103. Plaintiff Rogers suffered actual injury and damages in paying money to and using services from Defendant during the Data Breach that she would not have paid or ordered had Defendant disclosed that it lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Defendant provided timely and accurate notice of the Data Breach.

104. Plaintiff Rogers suffered actual injury in the form of damages to and diminution in the value of her personal and financial information – a form of intangible property that the Plaintiff Rogers entrusted to Defendant for the purpose of making purchases on its website and which was compromised in, and as a result of, the Data Breach.

105. Plaintiff Rogers suffers present and continuing injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by her personal and financial information being placed in the hands of criminals who have already misused such information stolen in the Data Breach.

106. Plaintiff Rogers has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected, and safeguarded from future breaches.

107. As a result of the Data Breach, Plaintiff Rogers made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff

Rogers has spent approximately one hour so far dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities.

108. As a result of the Data Breach, Plaintiff Rogers has suffered anxiety as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity crimes, fraud, and theft. Plaintiff Rogers is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

109. Plaintiff Rogers suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Rogers; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

110. As a result of the Data Breach, Plaintiff Rogers anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Rogers is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Silvia Cortez

111. Plaintiff Cortez was required to provide Defendant with her Private Information to access or activate her prepaid payment cards on Defendant's MyPrepaidCenter.com website.

112. Plaintiff Cortez suffered actual injury from having her Private Information compromised and/or stolen as a result of the Data Breach.

113. Plaintiff Cortez suffered actual injury and damages in paying money to and using services from Defendant during the Data Breach that she would not have paid or ordered had Defendant disclosed

that it lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Defendant provided timely and accurate notice of the Data Breach.

114. Plaintiff Cortez suffered actual injury in the form of damages to and diminution in the value of her personal and financial information – a form of intangible property that the Plaintiff Cortez entrusted to Defendant for the purpose of making purchases on its website and which was compromised in, and as a result of, the Data Breach.

115. Plaintiff Cortez suffers present and continuing injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by her personal and financial information being placed in the hands of criminals who have already misused such information stolen in the Data Breach.

116. Plaintiff Cortez has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected, and safeguarded from future breaches.

117. As a result of the Data Breach, Plaintiff Cortez made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff Cortez has spent approximately two hours so far dealing with the Data Breach, valuable time Plaintiff Cortez otherwise would have spent on other activities.

118. As a result of the Data Breach, Plaintiff Cortez has suffered anxiety as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity crimes, fraud, and theft. Plaintiff Cortez is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

119. Plaintiff Cortez suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Cortez; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

120. As a result of the Data Breach, Plaintiff Cortez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Cortez is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Sabrina Singleton's Experience

121. Plaintiff Singleton was required to provide Defendant with her Private Information to access or activate her prepaid payment cards on Defendant's MyPrepaidCenter.com website.

122. Plaintiff Singleton suffered actual injury from having her Private Information compromised and/or stolen as a result of the Data Breach.

123. Plaintiff Singleton suffered actual injury and damages in paying money to and using services from Defendant during the Data Breach that she would not have paid or ordered had Defendant disclosed that it lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Defendant provided timely and accurate notice of the Data Breach.

124. Plaintiff Singleton suffered actual injury in the form of damages to and diminution in the value of her personal and financial information – a form of intangible property that the Plaintiff Singleton entrusted to Defendant for the purpose of making purchases on its website and which was compromised in, and as a result of, the Data Breach.

125. Plaintiff Singleton suffers present and continuing injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by her personal and financial information being placed in the hands of criminals who have already misused such information stolen in the Data Breach. In fact, Plaintiff Singleton received a letter from the unemployment office informing her that it is investigating a claim for unemployment benefits.

126. Plaintiff Singleton has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected, and safeguarded from future breaches.

127. As a result of the Data Breach, Plaintiff Singleton made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff Singleton has spent approximately ten hours so far dealing with the Data Breach, valuable time Plaintiff Singleton otherwise would have spent on other activities.

128. As a result of the Data Breach, Plaintiff Singleton has suffered anxiety as a result of the release of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity crimes, fraud, and theft. Plaintiff Singleton is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

129. Plaintiff Singleton suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Defendant obtained from Plaintiff Singleton; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

130. As a result of the Data Breach, Plaintiff Singleton anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Singleton is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

Plaintiff Brian O'Connor's Experience

131. Plaintiff O'Connor was required to provide Defendant with her Private Information to access or activate her prepaid payment cards on Defendant's MyPrepaidCenter.com website.

132. Plaintiff O'Connor suffered actual injury from having his Private Information compromised and/or stolen as a result of the Data Breach.

133. Plaintiff O'Connor suffered actual injury and damages in paying money to and using services from Defendant during the Data Breach that he would not have paid or ordered had Defendant disclosed that it lacked computer systems and data security practices adequate to safeguard customers' personal and financial information and had Defendant provided timely and accurate notice of the Data Breach.

134. Plaintiff O'Connor suffered actual injury in the form of damages to and diminution in the value of his personal and financial information – a form of intangible property that the Plaintiff O'Connor entrusted to Defendant for the purpose of making purchases on its website and which was compromised in, and as a result of, the Data Breach.

135. Plaintiff O'Connor suffers present and continuing injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by his personal and financial information being placed in the hands of criminals who have already misused such information stolen in the Data Breach.

136. Plaintiff O'Connor has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected, and safeguarded from future breaches.

137. As a result of the Data Breach, Plaintiff O'Connor made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to, researching the Data Breach; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and researching credit monitoring and identity theft protection services offered by Defendant. Plaintiff O'Connor has spent several hours dealing with the Data Breach, valuable time Plaintiff O'Connor otherwise would have spent on other activities.

138. As a result of the Data Breach, Plaintiff O'Connor has suffered anxiety as a result of the release of his Private Information, which he believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of identity crimes, fraud, and theft. Plaintiff O'Connor is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting therefrom.

139. Plaintiff O'Connor suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Defendant obtained from Plaintiff O'Connor; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft and fraud.

140. As a result of the Data Breach, Plaintiff O'Connor anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff O'Connor is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ACTION ALLEGATIONS

141. Plaintiffs bring this nationwide class action on behalf of themselves, and all others similarly situated under Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

142. The Nationwide Class Plaintiffs seek to represent comprises:

All persons Defendant identified as being among those individuals impacted by the Data Breach, including all persons who were sent a notice of the Data Breach.

143. The California Subclass Plaintiffs seek to represent comprises:

All persons residing in California Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach (the "California Subclass").

144. The Illinois Subclass Plaintiffs seek to represent comprises:

All persons residing in Illinois Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach" (the "Illinois Subclass).

145. The Texas Subclass Plaintiffs seek to represent comprises:

All persons residing in Texas Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach (the "Texas Subclass").

146. The Colorado Subclass Plaintiffs seek to represent comprises:

All persons residing in Colorado Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach (the "Colorado Subclass").

147. The New York Subclass Plaintiffs seek to represent comprises:

All persons residing in New York Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach (the "New York Subclass").

148. The Mississippi Subclass Plaintiffs seek to represent comprises:

All persons residing in New York Defendant identified as being among those individuals impacted by the Data Breach, including those who were sent a notice of the Data Breach (the "New York Subclass").

149. Plaintiffs reserve the right to amend or modify the Class definitions and/or create additional subclasses as this case progresses.

150. Excluded from the Classes are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Classes are members of the judiciary to whom this case is assigned, their families, and Members of their staff.

151. **Numerosity**. The Members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Classes consist of at least 165,727[26] current and former customers of Defendant whose sensitive data was compromised in Data Breach.

152. **Commonality**. There are questions of law and fact common to the Classes, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

[26] See *Blackhawk Network Notice of Data Breach*, Oct. 31, 2022, archived by the Iowa Attorney General, *available at*: https://www.iowaattorneygeneral.gov/media/cms/10312022_Blackhawk_Engagement_Solut_1D9CB60967722.pdf (last accessed Nov. 8, 2022).

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant breached implied or express contracts with Plaintiffs and Class Members;

m. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiffs and Class Members;

n. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

o. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

153. **Typicality**. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

154. **Adequacy of Representation**. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class and has no interests antagonistic to those of other Class Members. Plaintiffs' counsels are competent and experienced in litigating Class actions.

155. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

156. **Superiority**. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

157. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and All Class Members)

158. Plaintiffs repeat and re-allege the allegations set forth in paragraphs 1-157 and incorporate the same as if set forth herein at length.

159. Defendant solicited and gathered the Private Information, including the PCD, of Plaintiffs and Class Members to facilitate sales transactions.

160. Defendant knew, or should have known, of the risks inherent in collecting Plaintiffs and the Class Members' Private Information and the importance of adequate security. Defendant also knew about numerous, well-publicized payment card data breaches involving other national retailers, including its own similar data breach from two years ago.

161. Defendant owed duties of care to Plaintiffs and the Class Members whose Private Information was entrusted to it. Defendant's duties included the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To exercise reasonable care in selecting its third-party vendors and monitoring and auditing their data security practices ensuring compliance with legal and industry standards and obligations;

c. To protect customers' Private Information using reasonable and adequate security procedures and systems that are compliant with the PCI DSS and consistent with industry-standard practices;

d. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

e. To promptly notify Plaintiffs and Class Members of the data breach.

162. By collecting this data and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property, to prevent disclosure of Private Information, and to safeguard the Private Information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in case of a data breach.

163. Defendant's duty of care extended to ensuring that any third-party vendors it hired and that had exposure to the Private Information of Plaintiffs and Class Members would implement adequate measures to prevent and detect cyber intrusions.

164. Because Defendant knew that a breach of its systems would damage thousands of its customers, including Plaintiffs and Class Members, it had a duty to adequately protect their Private Information.

165. Defendant owed a duty of care not to subject Plaintiffs and the Class Members to an unreasonable risk of harm because they were the foreseeable and probable victims of any inadequate security practices.

166. Defendant had a duty to implement, maintain, and ensure reasonable security procedures and practices to safeguard Plaintiffs' and Class Members' Private Information.

167. Defendant knew, or should have known, that its computer systems and security practices did not adequately safeguard the Private Information of Plaintiffs and the Class Members.

168. Defendant knew, or should have known, that the computer systems and security practices of its third-party vendors did not adequately safeguard the Private Information of Plaintiffs and the Class Members.

169. Defendant breached its duties of care by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and the Class Members.

170. Defendant breached its duties of care by failing to provide prompt notice of the data breach to the persons whose Private Information was compromised.

171. Defendant acted with reckless disregard for the security of the Private Information of Plaintiffs and the Class Members because Defendant knew or should have known that its computer

systems and data security practices, and those of its third-party vendors, were not adequate to safeguard the Private Information that that it collected, which hackers targeted in the Data Breach.

172. Defendant acted with reckless disregard for the rights of Plaintiffs and the Class Members by failing to provide prompt and adequate notice of the data breach so that they could take measures to protect themselves from damages caused by the fraudulent use the Private Information compromised in the data breach.

173. Defendant had a special relationship with Plaintiffs and the Class Members. Plaintiffs' and the Class Members' willingness to entrust Defendant with their Private Information was predicated on the mutual understanding that Defendant would implement adequate security precautions. Moreover, Defendant was in an exclusive position to protect its systems (and the Private Information) from attack. Plaintiffs and Class Members relied on Defendant to protect their Private Information.

174. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their Private Information. Defendant's misconduct included failing to:

a. Secure its e-commerce website;
b. Secure access to its and its vendors' servers;
c. Audit and monitor its vendors;
d. Comply with industry standard security practices;
e. Follow the PCI-DSS standards;
f. Encrypt PCD at the point-of-sale and during transit;
g. Employ adequate network segmentation;
h. Implement adequate system and event monitoring;
i. Utilize modern payment systems that provided more security against intrusion;
j. Install updates and patches in a timely manner; and
k. Implement the systems, policies, and procedures necessary to prevent this type of data breach.

175. Defendant also had independent duties under the FTC Act and state laws that required it to reasonably safeguard Plaintiffs' and the Class Members' Private Information and promptly notify them about the data breach.

176. Defendant breached the duties it owed to Plaintiffs and Class Members in numerous ways, including:

a. By creating a foreseeable risk of harm through the misconduct previously described;

b. By failing to implement adequate security systems, protocols, and practices sufficient to protect their Private Information both before and after learning of the Data Breach;

c. By failing to comply with the minimum industry data security standards, including the PCI-DSS, during the period of the Data Breach, and

d. By failing to timely and accurately disclose that Plaintiffs and Class Members Private Information had been improperly acquired or accessed.

177. But for Defendant's wrongful and negligent breach of the duties it owed Plaintiffs and the Class Members, their personal and financial information either would not have been compromised or they would have been able to prevent some or all of their damages.

178. As a direct and proximate result of Defendant's negligent conduct, Plaintiffs and the Class Members have suffered damages and are at imminent risk of further harm.

179. The injury and harm that Plaintiffs and Class Members suffered (as alleged above) was reasonably foreseeable.

180. The injury and harm that Plaintiffs and Class Members suffered (as alleged above) was the direct and proximate result of Defendant's negligent conduct.

181. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and All Class Members)

182. Plaintiffs repeat and re-allege the allegations set forth in paragraphs 1-157 and incorporate the same as if set forth herein at length.

183. When Plaintiffs and Class Members provided their Private Information to Defendant in making purchases on its website, they entered into implied contracts under which Defendant agreed to protect their Private Information and timely notify them in the event of a data breach.

184. Defendant invited its customers, including Plaintiffs and the Class, to make purchases of Prepaid Gift cards on its website using payment cards in order to increase sales by making purchases more convenient.

185. An implicit part of the offer was that Defendant would safeguard their Private Information using reasonable or industry-standard means and would timely notify Plaintiffs and Class Members in the event of a data breach.

186. Defendant also affirmatively represented in its Privacy Policy that it protected the Private Information of Plaintiffs and Class Members in several ways, as described above.

187. Based on the implicit understanding and also on Defendant's representations, Plaintiffs and Class Members accepted the offers and provided Defendant with their Private Information by using their payment cards in connection with purchases on the Defendant website during the period of the data breach.

188. Defendant manifested its intent to enter into an implied contract that included a contractual obligation to reasonably protect Plaintiffs' and Class Members' Private Information through, among other things, its Privacy Notice.

189. Defendant further demonstrated an intent to safeguard the Private Information of Plaintiffs and Class Members through its conduct. No reasonable person would provide sensitive, non-public information to a retailer without the implicit understanding that the retailer would maintain that information as confidential.

190. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

191. Plaintiffs and Class Members would not have provided their Private Information to Defendant had they known that Defendant would not safeguard their Private Information as promised or provide timely notice of a data breach.

192. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

193. Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' Private Information and failing to provide them with timely and accurate notice when their Private Information was compromised in the Data Breach.

194. The losses and damages Plaintiffs and Class Members sustained (as described above) were the direct and proximate result of Defendant's breaches of its implied contracts with them.

COUNT III
UNJUST ENRICHMENT
(on behalf of Plaintiffs and All Class Members)

195. Plaintiffs repeat and re-allege the allegations set forth in paragraphs 1-157 and incorporate the same as if set forth herein at length.

196. This claim is brought in the alternative to Plaintiffs' claim for breach of implied contract.

197. Defendant funds its data security measures entirely from its general revenue, including payments made by Plaintiffs and Class Members.

198. As such, a portion of the payments made by Plaintiffs and Class Members was to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

199. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they purchased goods (Prepaid Gift Cards, specifically) and services from Defendant and in so doing provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

200. Defendant knew that Plaintiffs and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

201. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information and instead directing those funds to its own profit. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

202. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

203. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

204. Plaintiffs and the Class have no adequate remedy at law.

205. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members of the Class conferred on it.

206. Defendant should be compelled to disgorge into a common fund or constructive trust for the benefit of Plaintiffs and Class Members proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and the Class overpaid, plus attorneys' fees, costs, and interest thereon.

COUNT IV
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW,
CAL. BUS. & PROF. CODE § 17200, *et seq*.
(On Behalf Plaintiffs and the California Subclass and Nationwide Class)

207. Plaintiffs repeat and re-allege the allegations set forth in paragraphs 1-157 and incorporate the same as if set forth herein at length.

208. For all Class members outside of the California, Illinois, Texas, Colorado, New York Subclasses, these claims are brought under the relevant consumer protection statute for the state in which they reside. For each state, the relevant statutes are as follows: Alabama-Deceptive Trade Practices Act (Ala. Code. § 8-19-1 et seq.); Alaska—Unfair Trade Practices and Consumer Protection Act (Alaska Stat. § 45.50.471, et seq.); Arizona—Consumer Fraud Act (Ariz. Rev. Stat. Ann. § 44-1521, et seq.); Arkansas—Deceptive Trade Practices Act (Ark. Code Ann. § 4-88-101, et seq.); Connecticut—Connecticut Unfair Trade Practices Act (Conn. Gen. Stat. § 42-110a, et seq.); Delaware—Consumer Fraud Act (Del. Code Ann. Tit. 6, § 2511, et seq.); District of Columbia— D.C. Code § 28-3901, et seq.; Florida— Deceptive and Unfair Trade Practices Act (Fla. Stat. § 501.20, et seq.); Georgia – Fair Business Practices Act of 1975 (Ga. Code § 10-1-390 et seq.);Hawaii—Haw. Rev. Stat. § 480-1, et seq.); Idaho—Consumer Protection Act (Idaho Code Ann. § 48-601, et seq.); Indiana—Deceptive Consumer Sales Act (Ind. Code § 24-5-0.5-1, et seq.); Iowa—Iowa Code § 7.14.16, et seq.); Kansas—Consumer Protection Act (Kan. Stat. Ann. § 50-623, et seq.); Kentucky—Consumer Protection Act (Ky. Rev. Stat. Ann. §

367.110, et seq.); Louisiana—Unfair Trade Practices and Consumer Protection Law (La. Rev. Stat. Ann. § 51:1401, et seq.); Maine–Unfair Trade Practices Act (Me. Stat. tit. 5, § 205-A ET SEQ.); (Maryland—Maryland Consumer Protection Act (Md. Code Ann., Com. Law § 13-101, et seq.); Massachusetts—Regulation of Business Practice and Consumer Protection Act (Mass. Gen. Laws Ann. ch. 93A, §§ 1-11); Minnesota—False Statement in Advertising Act (Minn. Stat. § 8.31, Minn. Stat. § 325F.67), Prevention of Consumer Fraud Act (Minn. Stat. § 325F.68, et seq.); Mississippi—Consumer Protection Act (Miss. Code Ann. § 75-24, et seq.); Missouri—Merchandising Practices Act (Mo. Rev. Stat. § 407.010, et seq.); Montana – Unfair Trade Practices and Consumer Protection Act of 1973 (Mont. Code Ann. § 30-14-101 et seq.); Nebraska—Consumer Protection Act (Neb. Rev. Stat. § 59-1601); Nevada—Trade Regulation and Practices Act (Nev. Rev. Stat. § 598.0903, et seq., Nev Rev. Stat. § 41.600); New Hampshire—Consumer Protection Act (N.H. Rev. Stat. Ann. § 358-A:1, et seq.); New Jersey—N.J. Stat. Ann. § 56:8-1, et seq.); New Mexico— Unfair Practices Act (N.M. Stat. § 57-12-1, et seq.); North Carolina (N.C. Gen. Stat. § 75-1.1 et seq.); North Dakota—N.D. Cent. Code § 51-15-01, et seq.); Ohio – Ohio Consumer Sales Practices Act (Ohio Rev. Code Ann. § 1345.01 ET SEQ.); Oklahoma—Consumer Protection Act (Okla. Stat. tit. 15, § 751, et seq.); Oregon—Unlawful Trade Practices Law (Or. Rev. Stat. § 646.605, et seq.); Rhode Island—Unfair Trade Practice and Consumer Protection Act (R.I. Gen. Laws § 6-13.1-1, et seq.); South Carolina—Unfair Trade Practices Act (S.C. Code Ann. § 39-5-10, et seq.); South Dakota—Deceptive Trade Practices and Consumer Protection Law (S.D. Codified Laws § 37-24-1, et seq.); Tennessee—Consumer Protection Act(Tenn. Code Ann. § 47- 18-101, et seq.); Utah—Consumer Sales Practices Act (Utah Code Ann. § 13-11-1, et seq.); Vermont—Consumer Fraud Act (Vt. Stat. Ann. tit. 9, § 2451, et seq.); Virginia-Consumer Protection Act of 1997 (Va. Code Ann. § 59.1-196 et seq.); Washington—Consumer Protection Act (Wash. Rev. Code § 19.86.010, et seq.); West Virginia-Consumer Credit and Protection Act (W. Va. Code § 46A-6-101 et seq.); Wisconsin— Wis. Stat. § 100.18, 100.20; Wyoming—Consumer Protection Act (Wyo. Stat. Ann. § 40-12-101, et seq.)

"Unfair" Prong

209. Under California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 et seq., a challenged activity is "unfair" when "any injury it causes outweighs any benefits provided to consumers and the injury is one that the consumers themselves could not reasonably avoid." Camacho v. Auto Club of Southern California, 142 Cal. App. 4th 1394, 1403 (2006).

210. Defendant's conduct as alleged herein does not confer any benefit to consumers. It is especially questionable why Defendant would continue to store individuals' data longer than necessary. Mishandling this data and a failure to archive and purge this unnecessary data shows blatant disregard for customers' privacy and security.

211. Defendant did not need to collect the private data from its consumers to allow consumers' enhanced experiences of the products or services. It did so to track and target its customers and monetize the use of the data to enhance its profits. Defendant utterly misused this data and Private Information.

212. Defendant's conduct as alleged herein causes injuries to consumers, who do not receive a service consistent with their reasonable expectations.

213. Defendant's conduct as alleged herein causes injuries to consumers, who entrusted Defendant with their Private Information and whose Private Information was leaked as a result of Defendant's unlawful conduct.

214. Defendant's failure to implement and maintain reasonable security measures was also contrary to legislatively declared public policy that seeks to protect consumers' data and ensure entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code §1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

215. Consumers cannot avoid any of the injuries caused by Defendant's conduct as alleged herein.

216. The injuries caused by Defendant's conduct as alleged herein outweigh any benefits.

217. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes an unfair business practice within the meaning of Cal. Bus. & Prof. Code § 17200.

218. Defendant could have furthered its legitimate business interests in ways other than by unfair conduct.

219. Defendant's conduct threatens consumers by exposing consumers' Private Information to hackers. Defendant's conduct also threatens other companies, large and small, who play by the rules. Defendant's conduct stifles competition and has a negative impact on the marketplace and reduces consumer choice.

220. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's wrongful conduct is part of a pattern or generalized course of conduct.

221. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs and the Class Members seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unfair business practices.

222. Plaintiffs and the Class Members have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs relied on and made their decision to use Defendant's services in part based on Defendant's representations regarding their security measures and trusted that Defendant would keep their Private Information safe and secure. Plaintiffs accordingly provided their Private Information to Defendant reasonably believing and expecting that their Private Information would be safe and secure. Plaintiffs paid an unwarranted premium for the purchased services. Specifically, Plaintiffs paid for services advertised as secure when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiffs and the Class Members would not have purchased the services, or would not have given Defendant their Private

Information, had they known that their Private Information was vulnerable to a data breach. Likewise, Plaintiffs and the members of the Class seek an order mandating that Defendant implement adequate security practices to protect consumers' Private Information. Additionally, Plaintiffs and the Class Members seek and request an order awarding Plaintiffs and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

"Unlawful" Prong

223. Cal. Bus. & Prof. Code § 17200, et seq., identifies violations of any state or federal law as "unlawful practices that the unfair competition law makes independently actionable." *Velazquez v. GMAC Mortg. Corp.*, 605 F. Supp. 2d 1049, 1068 (C.D. Cal. 2008).

224. Defendant's unlawful conduct, as alleged in the preceding paragraphs, violates Cal. Bus. & Prof. Code § 1750 et seq.

225. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes unlawful conduct.

226. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C. § 45, and California common law. Defendant failed to notify all of its affected customers regarding said breach, failed to take reasonable security measures, or comply with the FTC Act, and California common law.

227. Defendant knew or should have known of its unlawful conduct.

228. As alleged in the preceding paragraphs, the misrepresentations by Defendant detailed above constitute an unlawful business practice within the meaning of Cal. Bus. & Prof. Code §17200.

229. Defendant could have furthered its legitimate business interests in ways other than by its unlawful conduct.

230. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's unlawful conduct is part of a pattern or generalized course of conduct.

231. Pursuant to Cal. Bus. & Prof. Code § 17203, Plaintiffs and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unlawful business practices.

232. Plaintiffs and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs paid an unwarranted premium for services. Specifically, Plaintiffs paid for services advertised as secure when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiffs and the Class Members would not have purchased the products and services, or would not have given Defendant their Private Information, had they known that their Private Information was vulnerable to a data breach. Likewise, Plaintiffs and the members of the Class seek an order mandating that Defendant implement adequate security practices to protect consumers' Private Information. Additionally, Plaintiffs and the Class Members seek and request an order awarding Plaintiffs and the Class Members restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

COUNT V
VIOLATION OF CALIFORNIA'S CONSUMER PRIVACY ACT ("CCPA"),
CAL. CIV. CODE § 1798.150, *et seq*.
(On Behalf of the California Subclass)

233. Plaintiff O'Connor repeats and re-alleges the allegations set forth in paragraphs 1-157 and incorporates the same as if set forth herein at length.

234. Defendant is a corporation organized or operated for the profit or financial benefit of its owners with annual gross revenues in excess of $25,000,000.

235. Defendant collects consumers' personal information as defined in Cal. Civ. Code § 1798.140.

236. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiff O'Connor's and the California Subclass Members' nonencrypted Personal Information from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

237. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff O'Connor's and California Subclass Members' Private Information. As detailed herein, Defendant failed to do so. Specifically, Defendant's code left open a vulnerability that was used for unauthorized access and exfiltration, theft or disclosure of Plaintiff O'Connor's and California Subclass Member's Personal Information.

238. As a direct and proximate result of Defendant's acts, Plaintiff O'Connor's, and California Sub-Class Members' Personal Information, as defined in Cal. Civ. Code § 1798.81.5(d)(1)(A), including first and last name, email address, phone numbers, card numbers, expiration dates, and CVV security codes, was subjected to unauthorized access and exfiltration, theft, or disclosure.

239. Plaintiff O'Connor and California Sub-Class Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards customers' Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' Private Information, including Plaintiff O'Connor's and California Sub-Class Members' Private Information. Plaintiff O'Connor and California Sub-Class Members have an interest in ensuring that their Private Information is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information, as evidenced by its multiple data breaches.

240. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the Personal Information under the CCPA.

241. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant and third parties with similar inadequate security measures.

242. Plaintiff O'Connor and the California Sub-Class seek actual pecuniary damages, including actual financial losses resulting from the unlawful data breach.

243. On November 18, 2022, Plaintiff O'Connor provided Defendant with written notice by certified mail of Defendant's violations of the CCPA, pursuant to Civil Code § 1798.150(b)(1). Defendant responded to Plaintiff O'Connor's notice on December 15, 2022.

244. Defendant did not actually cure the noticed violations. Defendant asserted, without evidence or proof, that it "cured" the above failures to implement reasonable security procedures to prevent unauthorized access of Plaintiff O'Connor's and California Sub-Class Members' PII by discussing the post attack actions it allegedly took, which did not retroactively cure the unauthorized access, as they provide no assurance that Plaintiff O'Connor's and California Sub-Class members' PII is not still in the hands of unauthorized third parties.

245. Furthermore, none of the steps Defendant asserts in its response demonstrate an actual cure of its failure to implement reasonable security measures to protect Plaintiff O'Connor's and California Sub-Class members' PII as the steps it asserts it has taken are not sufficient to protect Plaintiff O'Connor's and California Sub-Class members' PII.

246. Defendant's response is wholly insufficient to demonstrate any "actual cure" of its failure to implement reasonable security to protect the information.

247. As Defendant has not "actually cured" the violation, Plaintiff O'Connor and the California Sub-Class seek statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(a)(1)(A) & (b).

COUNT VI
DECEIT BY CONCEALMENT,
CAL. CIV. CODE §§ 1709 AND 1710
(On Behalf of the California Sub-Class)

248. Plaintiff O'Connor repeats and re-alleges the allegations set forth in paragraphs 1-157 and incorporates the same as if set forth herein at length.

249. Defendant knew or should have known that its security systems were inadequate to protect the Private Information of its consumers. Defendant experienced another data breach just a few years prior to the breach at issue, which alerted Defendant to the inadequacy of its internal data protections. Despite this knowledge, Defendant failed to address the inadequacies in its security systems, and allowed the second breach to occur, this time compromising consumer's Private Information. Further, the August 2020 data breach included names, email addresses, postal addresses, the names and contact information of any gift card recipient(s). The leak of this source code should have put Defendant on further notice that the data of its account holders was at imminent risk.

250. Specifically, Defendant had an obligation to disclose to its consumers that its security systems were not adequate to safeguard their Private Information. Defendant did not do so. Rather, Defendant deceived Plaintiff O'Connor and the California Sub-Class by concealing the vulnerabilities in its security system.

251. Even after Defendant discovered the data breach, it concealed it, and waited over a month before announcing it to the public, thereby preventing them from taking precautions against the data breach.

252. Cal. Civ. Code § 1710 defines deceit as, (a) "[t]he suggestion, as a fact, of that which is not true, by one who does not believe it to be true"; (b) "[t]he assertion, as a fact, of that which is not true, by one who has no reasonable ground for believing it to be true"; (c) "[t]he suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for

want of communication of that fact"; or (d) "[a] promise, made without any intention of performing it." Defendant's conduct as described herein therefore constitutes deceit of Plaintiff O'Connor and the California Sub-Class.

253. Cal. Civ. Code § 1709 mandates that in willfully deceiving Plaintiff O'Connor and the California Sub-Class with intent to induce or alter their position to their injury or risk, Defendant is liable for any damage which Plaintiff O'Connor and the California Sub-Class thereby suffer.

254. As described above, Plaintiff O'Connor and the California Sub-Class have suffered significant harm as a direct and proximate result of Defendant's deceit and other unlawful conduct. Specifically, Plaintiff O'Connor and the California Sub-Class have been subject to numerous attacks, increase in spam phone calls and emails. Defendant is liable for these damages.

COUNT VII
VIOLATION OF ILLINOIS' CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, 805 ILL. COMP. STAT. 505/1, *et seq*.
(On Behalf of the Illinois Sub-Class)

255. Plaintiff Rogers repeats and re-alleges the allegations set forth in paragraphs 1-157 and incorporate the same as if set forth herein at length.

256. Plaintiff Rogers, Illinois Sub-Class members, and Defendant are "persons" as defined by 805 Ill. Comp. Stat. 505/1(c).

257. Defendant advertised, offered, or sold goods or services in Illinois and engaged in trade or commerce directly or indirectly affecting the people of Illinois, as defined by 805 Ill. Comp. Stat. 505/1(f).

258. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of 805 Ill. Comp. Stat. 505/2 and 805 Ill. Comp. Stat. 510/2, including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

259. Defendant's unfair, unconscionable, and deceptive practices include:

260. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Rogers' and Illinois Sub-Class members' Private Information, which was a direct and proximate cause of the data breach;

261. Failing to identify and remedy foreseeable security and privacy risks and adequately improve security systems despite knowing not only the general risk of cybersecurity incidents, but also the specific vulnerability of Defendant's systems, having been breached just a few years earlier;

262. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Rogers' and Illinois Sub-Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

263. Failing to appropriately delete or erase data that was no longer required to be stored, so as not to unnecessarily risk consumers' Private Information;

264. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Rogers' and Illinois Sub-Class members' Private Information, including by implementing and maintaining reasonable security measures;

265. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Rogers' and Illinois Sub-Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

266. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Rogers' and Illinois Sub-Class members' Private Information; and

267. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Rogers' and Illinois Sub-Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

268. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security systems and ability to protect consumers' Private Information.

269. Defendant intended to mislead Plaintiff Rogers and Illinois Sub-Class members and induce them to rely on its own misrepresentations and omissions.

270. Defendant also failed to implement and maintain reasonable security measures to protect Plaintiff Rogers and Illinois Sub-Class members' Private Information from unauthorized access, acquisition, destruction, use, modification, or disclosure, in violation of 805 Ill. Comp. Stat. 530/45.

271. Defendant acted intentionally, knowingly, and maliciously to violate 805 Ill. Comp. Stat. 505/2 and 805 Ill. Comp. Stat. 510/2, and recklessly disregarded Plaintiff Rogers' and Illinois Sub-Class members' rights. Defendant's recent 2020 Data Breach put it on notice that its security and privacy protections were inadequate.

272. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiff Rogers and Illinois Sub-Class members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their

financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Defendant's products and services; and the value of identity protection services made necessary by the data breach.

273. Plaintiff Rogers and the Illinois Sub-Class members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, reasonable attorneys' fees, and any other relief that is just and proper.

COUNT VIII
VIOLATION OF TEXAS'S DECEPTIVE TRADE PRACTICES – CONSUMER PROTECTION ACT, TEX. BUS. & COM. CODE ANN. §17.41, *et seq*.
(On Behalf of the Texas Sub-Class)

274. Plaintiff Cortez repeats and re-alleges the allegations set forth in paragraphs 1-157 and incorporates the same as if set forth herein at length.

275. Plaintiff Cortez, Texas Sub-Class members, and Defendant are "persons" as defined by Tex. Bus. & Com. Code Ann. § 17.45(2).

276. Defendant advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code Ann. § 17.45(6).

277. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Tex. Bus. & Com. Code Ann. § 17.46, including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

278. Defendant's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Cortez's and Texas Sub-Class members' Private Information, which was a direct and proximate cause of the data breach;

b. Failing to identify and remedy foreseeable security and privacy risks and adequately improve security systems despite knowing not only the general risk of cybersecurity incidents, but also the specific vulnerability of Defendant's systems, having been breached just a few years earlier;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Cortez's and Texas Sub-Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

d. Failing to appropriately delete or erase data that was no longer required to be stored, so as not to unnecessarily risk consumers' Private Information;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Cortez's and Texas Sub-Class members' Private Information, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Cortez's and Texas Sub-Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Cortez's and Texas Sub-Class members' Private Information; and

h. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Cortez's and Texas Sub-Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

279. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security systems and ability to protect consumers' Private Information.

280. Defendant intended to mislead Plaintiff Cortez and Texas Sub-Class members and induce them to rely on its own misrepresentations and omissions.

281. Defendant acted intentionally, knowingly, and maliciously to violate Tex. Bus. & Com. Code Ann. § 17.41 et seq., and recklessly disregarded Plaintiff Cortez's and Texas Sub-Class members' rights. Defendant's recent 2020 Data Breach put it on notice that its security and privacy protections were inadequate.

282. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiff Cortez and Texas Sub-Class members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of

value of their Private Information; overpayment for Defendant's products and services; and the value of identity protection services made necessary by the data breach.

283. Plaintiff Cortez and the Texas Sub-Class members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, reasonable attorneys' fees, and any other relief that is just and proper.

COUNT IX
VIOLATION OF COLORADO CONSUMER PROTECTION ACT
Colo. Rev. Stat. § 6-1-101, et seq.
(On the Colorado Sub-Class)

284. Plaintiff Pryor repeats and re-alleges the allegations set forth in paragraphs 1-157 and incorporates the same as if set forth herein at length.

285. The Colorado Consumer Protection Act ("Colorado CPA"), Colo. Rev. Stat. § 6-1-105(1)(l), et seq., prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service.

286. Defendant is a "person" under § 6-1-102(6) of the Colorado CPA, Colo. Rev. Stat. § 6-1-101, et seq.

287. Plaintiff Pryor and Colorado Sub-Class members provided and/or entrusted sensitive and confidential Private Information to Defendant, which Defendant collected, stored, and maintained.

288. Defendant is engaged in, and its acts and omissions affect, trade and commerce. Defendant's relevant acts, practices, and omissions complained of in this action were done in the course of Defendant's business of marketing, offering for sale, and selling goods and services throughout Colorado and the United States.

289. In the conduct of its business, trade, and commerce, Defendant engaged in the conduct alleged in this Complaint in transactions intended to result, and which did result, in the provision or sale of services to consumers. Plaintiff Pryor and Colorado Sub-Class members furnished or purchased these

services. Plaintiff Pryor and Colorado Sub-Class members are actual or potential consumers as defined by Colo. Rev. Stat § 6-1-113(1), et seq.

290. In the conduct of its business, trade, and commerce, Defendant collected and stored highly personal and private information, including Private Information belonging to Plaintiff Pryor and Colorado Sub-Class members.

291. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Private Information of Plaintiff Pryor and Colorado Sub-Class members, and that the risk of a data breach was highly likely and/or that the risk of the data breach being more extensive than originally disclosed was highly likely.

292. Defendant should have disclosed this information regarding its computer systems and data security practices because Defendant was in a superior position to know the true facts related to its security practices, and Plaintiff Pryor and Colorado Sub-Class members could not reasonably be expected to learn or discover the true facts.

293. As alleged herein this Complaint, Defendant engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and the furnishing of customer relation services to consumers in violation of the Colorado CPA, including but not limited to the following:

a. failing to adequately secure Plaintiff Pryor's and Colorado Sub-Class members' Private Information;

b. failing to maintain adequate computer systems and data security practices to safeguard Plaintiff Pryor's and Colorado Sub-Class members' Private Information;

c. failing to disclose the material information, known at the time of the transaction—collection and retention of Plaintiff Pryor's and Colorado Sub-Class members' Private Information to furnish customer relation services—that its computer systems would not

adequately protect and safeguard Plaintiff Pryor's and Colorado Sub-Class members' Private Information;

d. inducing Plaintiff Pryor and Colorado Sub-Class members to use Defendant's services by failing to disclose, and misrepresenting the material fact that, Defendant's computer systems and data security practices were inadequate to safeguard Plaintiff Pryor's and Colorado Sub-Class members' sensitive personal information from theft.

294. By engaging in the conduct delineated above, Defendant has violated the Colorado CPA by, among other things:

a. omitting material facts regarding the goods and services sold;

b. omitting material facts regarding the security of the transactions between Defendant and Plaintiff Pryor and Colorado Sub-Class members;

c. omitting material facts regarding the security of the transactions between Defendant and Plaintiff Pryor and Colorado Sub-Class members who furnished or entrusted their Personal Information;

d. misrepresenting material facts in the furnishing or sale of products, goods, or services to Plaintiff Pryor and Colorado Sub-Class members;

e. engaging in conduct that is likely to mislead Plaintiff Pryor and Colorado Sub-Class members acting reasonably under the circumstances;

f. engaging in conduct that creates a likelihood of confusion or of misunderstanding;

g. engaging in conduct with the intent to induce Plaintiff Pryor and Colorado Sub-Class members to use Defendant's service;

h. unfair practices that caused or were likely to cause substantial injury to consumers that is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to Plaintiff Pryor and Colorado Sub-Class members; and/or

i. other unfair, deceptive, unconscionable, fraudulent and/or unlawful acts or practices to be shown at trial.

295. Defendant systemically engaged in these deceptive, misleading, and unlawful acts and practices, to the detriment of Plaintiff Pryor and Colorado Sub-Class members.

296. Defendant's actions in engaging in the conduct delineated above were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiff Pryor and Colorado Sub-Class members.

297. As a direct result of Defendant's violation of the Colorado CPA, Plaintiff Pryor and Colorado Sub-Class members have suffered actual damages, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect that Private Information; and (viii) present and future costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information

compromised as a result of the Data Breach for the remainder of the lives of Plaintiff Pryor and Colorado Sub-Class members.

298. As a result of Defendant's violation of the Colorado CPA, Plaintiff Pryor and Colorado Sub-Class members are entitled to, and seek, injunctive relief, including, but not limited to:

a. Ordering that Defendant engage third-party security auditors/penetration testers as well as experienced and qualified internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendant engage third-party security auditors and experienced and qualified internal security personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train its security personnel regarding new or modified procedures;

d. Ordering that Defendant segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner employee and customer data not necessary for its provision of services;

f. Ordering that Defendant conduct regular database scanning and securing checks;

g. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and,

h. Ordering Defendant to meaningfully educate its employees and customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps customers must take to protect themselves.

299. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices of Defendant alleged herein, Plaintiff Pryor and Colorado Sub-Class members seek relief under Colo. Rev. Stat. § 6-1-113, including, but not limited to, the greater of actual damages, statutory damages, or treble damages for bad faith conduct, injunctive relief, attorneys' fees and costs, as allowable by law.

COUNT X
VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 349
(On the New York Sub-Class)

300. Plaintiff Singleton and the New York Sub-Class repeat and re-allege the allegations set forth in paragraphs 1-157 and incorporate the same as if set forth herein at length.

301. Defendant engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Singleton's and New York Sub-Class members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately maintain and/or improve security and privacy measures, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Singleton's and New York Sub-Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, et seq., which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Singleton's and New York Sub-Class members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Singleton's and New York Sub-Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, et seq.;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Singleton's and New York Sub-Class members' Private Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Singleton's and New York Sub-Class members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, et seq.

302. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Private Information.

303. Defendant acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff Singleton's and New York Sub-Class members' rights.

304. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff Singleton and New York Sub-Class members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent

activity, an increased, imminent risk of fraud and identity theft and loss of value of their Private Information.

305. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the thousands of New Yorkers and New York businesses affected by the Data Breach.

306. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff Singleton and New York Sub-Class members that they could not reasonably avoid.

307. Plaintiff Singleton and New York Sub-Class members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. An Order certifying the Classes, and appointing Plaintiffs and their Counsel to represent the Classes;

B. Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

C. Injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order;

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected

through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's

final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. An award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. Prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Date: February 9, 2023

Respectfully Submitted,

/s/ M. Anderson Berry

M. Anderson Berry (SBN 262879)
aberry@justice4you.com
Gregory Haroutunian (SBN 330263)
gharoutunian@justice4you.com
CLAYEO C. ARNOLD,
A PROFESSIONAL CORPORATION
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916)239-4778
Fax: (916) 924-1829

Terence R. Coates (*pro hac vice*)
tcoates@msdlegal.com
Justin C. Walker (*pro hac vice*)
jwalker@msdlegal.com
Dylan J. Gould (*pro hac vice*)
dgould@msdlegal.com
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Telephone: (513) 651-3700
Fax: (513) 665-0219

Marcus J. Bradley, Esq (SBN 174156)
mbradley@bradleygrombacher.com
Kiley L. Grombacher, Esq. (SBN 245960)

kgrombacher@bradleygrombacher.com
Lirit A. King, Esq. (SBN 252521)
lking@bradleygrombacher.com
BRADLEY/GROMBACHER LLP
31365 Oak Crest Drive, Suite 240
Westlake Village, CA 91361
Telephone: (805) 270-7100

Scott Edward Cole (SBN 160744)
sec@colevannote.com
Laura Grace Van Note (SBN 310160)
lvn@colevannote.com
Code Alexander Bolce (SBN 322725)
cab@colevannote.com
COLE & VAN NOTE
555 12th Street, Suite 1725
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: sec@colevannote.com
Email: lvn@colevannote.com
Email: cab@colevannote.com

Attorneys for Plaintiffs and the Proposed Classes